REMARKS

Claims 1-75 are currently pending in the subject application and are presently under consideration. Claims 1, 3-7, 14, 22, 23, 27, 28, 35, 38, 47, 48, 53, 54, 61, 65, 71, 73, 74 and 75 have been amended as shown at pages 2-14. In addition, claim 70 has been cancelled.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-75 Under 35 U.S.C. §102(e)

Claims 1-75 stand rejected under 35 U.S.C. §102(e) as being anticipated by Bates (US 6,779,021). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Bates, *et al.* does not teach or suggest each and every limitation of appellants' claimed invention.

> For a prior art reference to anticipate, 35 U.S.C. §102 requires that "each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950 (Fed. Cir. 1999) (*quoting Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631, 2USPQ2d 1051, 1053 (Fed. Cir. 1987)).

The subject application relates to identification of spam and spam senders at the sender's outgoing message system, and for increasing costs or preventing sending outgoing spam. For example, the system can perform various counts and compute various scores in order to detect spam senders, as well as, force e-mail senders to perform additional steps or pay fees when they are identified as a potential spam sender. In particular, independent claim 1 recites *a detection component employed by an outgoing message server that detects a potential spammer in connection with at least one outgoing message sent by an entity, the detection of a potential spammer being based in part on a total score per sender assigned to the entity of the at least one outgoing message exceeding a threshold score indicative of a spammer; and an action component that upon receiving information from the detection component that the entity is a potential spammer initiates at least one action to mitigate spam from the potential spammer, wherein* ***the at least one action includes limiting sending of outgoing messages by the entity to a specified volume of outgoing messages until a subset of the at least one outgoing message***

are manually inspected by a human inspector and confirmed by the human inspector as not being spam.

Bates, *et al.* does not teach or suggest the aforementioned novel aspects of the subject claims. The cited reference discloses a system that is primarily concerned with detection of spam at a recipient's system. The system employs various filters that are based upon counts or keywords in the message in order to determine spam. However, the reference fails to disclose limiting sending volume of outgoing messages to a specified volume until certain outgoing messages are inspected manually by a human to confirm that they are not spam. This advantageously allows a non-spammer who is sending legitimate mail that appears like spam to continue to send messages while a human verifies that they are not sending spam. For example, a person may be sending out a newsletter with a substantial number of hyperlinks to a significant number of recipients. This newsletter may appear like spam to an automated spam detection system, but is actually legitimate. The feature of the subject claim can avoid disrupting the person's ability to send messages. Bates, *et al.* is silent regarding this feature and, therefore, fails to teach or suggest *an action component that upon receiving information from the detection component that the entity is a potential spammer initiates at least one action to mitigate spam from the potential spammer, wherein* ***the at least one action includes limiting sending of outgoing messages by the entity to a specified volume of outgoing messages until a subset of the at least one outgoing message are manually inspected by a human inspector and confirmed by the human inspector as not being spam***.

Claim 4 recites *the detection component* ***increases the threshold score for the entity upon confirmation that the subset of the at least one outgoing message is not spam***. The subject claims allows for adjustment to the threshold upon confirming that the message were not spam. Using the example above, the system can adjust the threshold such that in the future a newsletter may not trigger an indication of potential spam for this person.

Claim 14 recites ***a number of apparently legitimate outgoing messages is used as a bonus in the total score per sender to offset one or more other scores applied in the total score per sender, wherein the one or more other scores are based upon one or more other indications of spam***. A non-spammer may send messages that appear like spam. The subject claim recites a feature whereby messages that appear legitimate are used to offset spam-like messages in the total score per sender used to identify potential spammers. This can, for

example, advantageously provide another mechanism to avoid disruption of sending outgoing messages by an entity that is not sending spam, but may occasionally send a message that appears like spam. The cited reference is silent regarding this novel feature recited in claim 14.

Claim 17 recites ***the total score per sender is based upon a number of non-deliverable messages of the at least one outgoing message***. Contrary to assertions in the Office Action, Bates, *et al.* is silent regarding determining a number of non-deliverable massages sent by an entity. The cited section, column 7, lines 23-47, discusses receipt of messages at an incoming e-mail server where a large number of users are receiving the same or similar messages. At this point the messages have been delivered at the recipient server. An incoming e-mail server is not able to determine a number of non-deliverable messages sent from an entity based upon an e-mail that the incoming e-mail server has received from the entity. The entity can send outgoing messages that are received by many different incoming e-mail servers. The subject claim, based upon its dependence to claim 1 discloses the outgoing message server performing the detection based total score per sender. Bates, *et al.* is only focused on the incoming e-mail server. As such, the cited reference fails to make obvious a total score per sender that is based upon a number of non-deliverable messages of the at least one outgoing message as recited in claim 17.

Claim 18 recites *wherein* ***the number of non-deliverable messages*** *is estimated at least in part from* ***Non Delivery Receipts***. Additionally, claims 19-21 recite various limitations related Non Delivery Receipts. The Office Action again cites column 7, lines 23-47 as teaching the limitations of these claims. On the contrary, this section merely discusses a number of users at an e-mail server receiving similar e-mails. Bates, *et al.* is silent regarding the number of non-deliverable messages and non delivery receipts at the outgoing message server and thus fails to teach all of the elements of claims 18-21.

Independent claim 35 recites *detecting a potential spammer in connection with at least one outgoing message, the* ***detection being based in part on at least one of number of apparently legitimate outgoing messages sent from the user account*** or ***number of non-deliverable messages sent from the user account***. The cited reference fails to disclose employing the number of legitimate outgoing messages or the number of non-deliverable messages from a sender in order to determine if the sender is sending spam. The cited reference relies upon generic counts of total outgoing messages or number of recipients in an e-mail message. The Office Action cites Figures 4A and 4B and column 8, line 48-column9, line 2 as

teaching the detection of a potential spammer being based in part on at least one of number of apparently legitimate outgoing messages sent from an entity's user account. On the contrary this particular section of the cited reference discloses an e-mail server receiving incoming e-mail and determining if the e-mail is spam based upon the number addressees in the e-mail. The number of addresses listed in a received e-mail is not equivalent to the number of apparently legitimate outgoing messages sent from an entity's user account. The reference is silent regarding tracking legitimate outgoing messages from a user account. E-mail being received by an e-mail server cannot be employed to determine number of outgoing messages from a user account. An entity could be sending many outgoing messages that are received by various recipient e-mail servers. Each of these recipient e-mail servers would not necessarily be aware of messages received by the other recipient e-mail servers. Also, for example, spammers often falsely employ other user's account information when sending e-mail that is actually not being sent from the other user's account in order to mislead recipients. Bates, *et al.* only discloses an incoming e-mail server analyzing incoming e-mails for spam. Therefore, Bates, *et al.* fails to teach or suggest *detecting a potential spammer in connection with at least one outgoing message, the* ***detection being based in part on at least one of number of apparently legitimate outgoing messages sent from an entity's user account*** or ***number of non-deliverable messages sent from the entity's user account***.

Furthermore, claim 38 recites ***computing a total score per sender based upon two or more of the score per outgoing message, the score per sender based at least in part upon outgoing message volume per sender, score per sender based at least in part upon outgoing message rate per sender, the a score per sender based at least in part upon a total recipient count per sender, or the score per sender based at least in part upon a unique recipient count per sender***. Bates, *et al.* discloses various counts but fails to teach combining the counts into a total score for a sender in order to determine if a sender is sending spam. Producing a combined score allows the various sub components of the total score to possibly offset each other, thereby reducing/increasing the influence of one particular component in determining a spam sender. Bates, *et al.* doesn't teach computing a total score per sender as recited in the subject claim. The Office Action dated November 30, 2007 asserts that the Abstract, column 4, lines 45-51, and column 7, lines 7-12 disclose this feature. On the contrary, the Abstract merely states that e-mails are analyzed and classified as potentially undesirable. Column 4, lines 45-51 and column

7, lines 7-12 states that a percentage of predictability of spam and a percentage of likelihood as spam respectively is determined for an e-mail message. However, these are not equivalent to computing a total score based upon at least two of *the score per outgoing message, the score per sender based at least in part upon outgoing message volume per sender, score per sender based at least in part upon outgoing message rate per sender, the a score per sender based at least in part upon a total recipient count per sender, or the score per sender based at least in part upon a unique recipient count per sender* as recited in the subject claim. The cited reference fails to discuss how these percentages are computed, and is silent regarding employing two or more of the specific scores recited in the subject claim to compute a total score. In addition, the Office Action dated September 19, 2008 fails to make a specific citation regarding the total score computation of the subject claim. Based upon the above reasoning, Bates, *et al.* fails to teach or all of the elements of the subject claim.

Additionally, independent claim 61 recites ***requiring an owner of the user account to resolve one or more challenges after at least one of a number of outgoing messages sent from the user account exceeds a predetermined threshold*** *or* ***a number of recipients counted in one or more sent messages from the user account exceeds a predetermined threshold; and suspending sending of subsequent outgoing messages from the user account until the one or more challenges are resolved***. Bates, *et al.* is silent regarding requiring the sender of a message to perform any kind of challenge in order to send messages. The cited reference discloses that users can be restricted from using their accounts to send spam. However, the reference fails to disclose that this restriction requires a user to solve a challenge after a number of outgoing messages sent from the user account exceeds a predetermined threshold or a number of recipients counted in one or more sent messages from the user account exceeds a predetermined threshold. The cited reference merely makes a general statement that a user account can be restricted without discussing any specifics related to the restriction. Therefore, the reference fails to teach all of the elements of claim 61.

Moreover, independent claim 65 (and similarly independent claim 75) recites *performing at least one economic analysis to determine sender outgoing message volume limit based at least in part on spammer behavior and legitimate user behavior; and* ***limiting the sender outgoing message volume to at least one of: a maximum number of unique recipients per challenge resolved, a maximum number of unique recipients per fee paid by a sender, a maximum***

number of outgoing messages per challenge resolved, or a maximum number of outgoing messages per fee paid by a sender. Bates, *et al.* is silent regarding performing any economic analysis, especially one in conjunction with determining sender outgoing message volume limits. The cited reference is also silent regarding resolving challenges and a message volume fee paid by a sender. As such, Bates, *et al.* fails to teach or suggest limiting the sender outgoing message volume to at least one of: a maximum number of unique recipients per challenge resolved, a maximum number of unique recipients per fee paid by a sender, a maximum number of outgoing messages per challenge resolved, or a maximum number of outgoing messages per fee paid by a sender.

Independent claim 71 recites *a detection component employed by an outgoing message server that detects a potential spammer in connection with at least one outgoing message sent from an account, the outgoing message comprising at least one of e-mail message spam, instant message spam, whisper spam, or chat room spam,* ***the detection component limits the account to a specified number of recipients or outgoing messages per challenge until a specified maximum number of challenges are solved, and after the specified maximum number of challenges are solved then the account is limited to a specified sending rate of a number of outgoing messages per time period, wherein the challenge is at least one of a human interactive proof or computational challenge***. The recited limitations disclose a feature that can add a cost to sending spam that is costly to spammers, while limiting inconvenience to a legitimate message sender. For example, a spam sender typically sends messages to a substantial number of recipients and sends a significant number of messages. Requiring the spammer to solved challenges based on number or recipients or messages can impose an upfront cost that is expensive to the user in relation to the subsequent sending rate limit that is imposed after a maximum number of challenges are solved. It is likely that the recipients of spam will inform an ISP or block the sender before the maximum number of challenges are solved. If the spammer tries to send legitimate messages prior to reaching the maximum number of challenges, the subsequent sending rate limit can make it cost ineffective to resolve the challenges. Bates, *et al.* is silent regarding the combination of challenge requirements and subsequent sending rate as recited in subject limitations and thus fails to teach make obvious the elements of claim 71.

Claim 47 recites ***the user account is limited to a specified number of recipients or outgoing messages per challenge until a specified maximum number of challenges are solved,***

and after the specified maximum number of challenges are solved then the account is limited to a specified sending rate of a number of outgoing messages per time period. Based on the reasoning discussed above with respect to independent claim 71, the cited reference also fails to teach the limitations of claim 47.

Independent claim 72 recites *information employed by an* ***outgoing message server*** *associated with detecting spam-like characteristics with at least one outgoing message, the outgoing message comprising at least one of instant message spam, whisper spam, and chat room spam,* ***the detection being based in part on at least one of number of apparently legitimate outgoing messages sent from an entity's user account*** *or* ***number of non-deliverable messages sent from the entity's user account****, wherein the information determines whether to initiate at least one action that facilitates any one of confirming that the entity is a spammer, mitigating spamming by the entity, or increasing spammer cost*. As noted *supra* with respect to independent claim 35, Bates, *et al*. fails to teach an outgoing e-mail server employing the number of legitimate outgoing messages or the number of non-deliverable messages from a sender in order to determine if the sender is sending spam. The cited sections of the reference relate to recipient counting at an incoming e-mail server, which does not allow for determining the number of apparently legitimate outgoing messages sent from an entity's user account. Hence, Bates, *et al*. does not teach all of the elements of claim 72.

Independent claim 73 recites *a means for initiating at least one action that facilitates mitigating spamming by the entity, wherein the at least one action includes* ***sending a legal notice to an owner of the account informing the owner that the account is in violation of at least one term of service of the account***. The subject claim recites a novel feature whereby an entity will be sent a legal notice indicating that their account is violating the terms of service of the account when the entity is determined to be a potential spammer. Bates, *et al*. is silent regarding this feature of the subject claim and thus fails to teach all of the limitations of claim 73.

Claim 53 recites *the at least one action comprises* ***sending a legal notice to the sender that the sender is in violation of terms of service*** *and suspending the account of the sender*. As discussed above, Bates, *et al*. fails to disclose sending a legal notice to a sender who is violating terms of service of an account and thus fails to make obvious the limitations of claim 53.

Claim 54 recites ***requiring the sender to respond to the legal notice acknowledging that the sender has read the legal notice prior to removing the suspension of the account via at least one of providing an electronic signature or clicking on a link***. Bates, *et al.* is silent regarding requiring a sender to provide an electronic acknowledgement that they have read a legal notice prior to removing the suspension of an account. As such, the reference fails to make obvious the limitations of claim 54.

Independent claim 74 recites *a means for* ***estimating a number of unique outgoing message recipients associated with outgoing messages sent from a user account***, *wherein the means for* ***estimating estimates the number of unique outgoing message recipients by computing a hash function per recipient to obtain a hash value per recipient, setting a hash modulo value, and adding a recipient to a list for message tracking when the recipient's hash value equals the hash modulo value to facilitate estimating a total volume of distinct recipients per sender***; *a means for* ***requiring an owner of the user account to resolve one or more challenges after the estimated number of unique outgoing message recipients exceeds a predetermined threshold***; *and a* ***means for suspending sending of subsequent outgoing messages until the one or more challenges are resolved***. The subject claim recites that unique recipients associated with outgoing messages is estimated using a hash function and a hash modulo value. This allows for a estimating the number of unique recipients without having to track each recipient. Bates, *et al.* fails to teach this novel feature for estimating unique recipients associated with outgoing messages. Moreover, as discussed above, the cited reference also does not disclose employing challenges or suspending outgoing messages until a challenge is resolved. Therefore, Bates, *et al.* fails to teach all elements of the subject claim.

In view of at least the above, it is respectfully submitted that Bates, *et al.* does not teach or suggest all limitations as recited in independent claims 1, 35, 61, 65, and 71-75 (and claims 2-34, 36-60, 62-64, and 66-69 which respectively depend there from) and thus fails to anticipate the subject claims. Accordingly, withdrawal of this rejection is respectfully requested.

II. Rejection of Claims 61-70 and 74 Under 35 U.S.C. §102(e)

Claims 61-70 and 74 stand rejected under 35 U.S.C. §102(e) as being anticipated by Wilson (US 2004/0015554). It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Wilson does not teach or suggest each and every limitation of

appellants' claimed invention.

Independent claim 61 recites ***requiring an owner of the user account to resolve one or more challenges after at least one of a number of outgoing messages sent from the user account exceeds a predetermined threshold*** *or* ***a number of recipients counted in one or more sent messages from the user account exceeds a predetermined threshold; and suspending sending of subsequent outgoing messages from the user account until the one or more challenges are resolved***.

Contrary to assertions in the Office Action, Wilson does not teach or suggest the aforementioned novel aspects of the subject claims. Cited figures 1, 2, 3, 5, Abstract, and paragraphs 61-63 of Wilson disclose identification of spam at a recipient's incoming mail system. The system employs an address filter to let through accepted addresses and send blocked addresses to a rejected folder. Unknown addresses cause a challenge to be sent to the sender to help validate the sender as legitimate or a spam sender. Senders who respond to the challenge correctly, are added to a list of allowed senders, and those that do not respond appropriately are added to a list of blocked senders. The cited reference relies on identifying spam at a recipient's incoming mail system, **where as the subject claims detect spam senders based upon the senders outgoing mail and take actions to suspend the senders account** when appropriate. The subject claim employs techniques to identify senders of spam at the sender's outgoing e-mail system and then based upon thresholds of outgoing message indicative of spam, will stop sending of outgoing messages until the sender has completed a challenge. In the system of Wilson, a sender is not restricted from sending messages in any way. Wilson is focused on the incoming e-mail server which does not have the ability to suspend outgoing messages from a user account of a sending address listed in an incoming e-mail.

Independent claim 65 recites *performing at least one economic analysis to determine sender outgoing message volume limit based at least in part on spammer behavior and legitimate user behavior; and* ***limiting the sender outgoing message volume to at least one of: a maximum number of unique recipients per challenge resolved, a maximum number of unique recipients per fee paid by a sender, a maximum number of outgoing messages per challenge resolved, or a maximum number of outgoing messages per fee paid by a sender***. Wilson does not disclose performing any economic analysis related to sender outgoing message volume limits. The cited reference is also silent regarding a fee paid by a sender. Wilson is concerned with detecting and

managing spam at an incoming e-mail server and does not discuss controlling outgoing message volume from a sender based upon challenges or fees. As such, the reference fails to teach or suggest limiting the sender outgoing message volume to at least one of: a maximum number of unique recipients per challenge resolved, a maximum number of unique recipients per fee paid by a sender, a maximum number of outgoing messages per challenge resolved, or a maximum number of outgoing messages per fee paid by a sender as recited in claim 65.

Moreover, independent claim 74 recites *a means for* ***estimating a number of unique outgoing message recipients associated with outgoing messages sent from a user account,*** *wherein the means for* ***estimating estimates the number of unique outgoing message recipients by computing a hash function per recipient to obtain a hash value per recipient, setting a hash modulo value, and adding a recipient to a list for message tracking when the recipient's hash value equals the hash modulo value to facilitate estimating a total volume of distinct recipients per sender****; a means for* ***requiring an owner of the user account to resolve one or more challenges after the estimated number of unique outgoing message recipients exceeds a predetermined threshold****; and a* ***means for suspending sending of subsequent outgoing messages until the one or more challenges are resolved***. Wilson fails is silent regarding estimating unique recipients associated with outgoing messages based upon a hash function and a hash modulo value as recited in the subject claim. As discussed *supra*, the cited reference also does not disclose restricting outgoing messages based upon a threshold number of outgoing messages until a challenge is resolved. Therefore, Wilson fails to teach all elements of the subject claim.

In view of at least the above, it is respectfully submitted that Wilson does not teach or suggest all limitations as recited in independent claims 61, 65 and 74 (and claims 62-69 which respectively depend there from) and thus fails to anticipate the subject claims. Accordingly, withdrawal of this rejection is respectfully requested.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP418US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Nilesh S. Amin/
Nilesh S. Amin
Reg. No. 58,407

AMIN, TUROCY & CALVIN, LLP
57TH Floor, Key Tower
127 Public Square
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731